## REMARKS

## INTRODUCTION

In accordance with the foregoing, claims 1, 7, 23, 29, 47 and 54 have been amended. Claims 52 and 53 have been cancelled. Claims 1-51, 54 and 55 are pending and under consideration.

## EXAMINER INTERVIEW

The Applicants extend their thanks to the Examiner for the courtesy shown to their representatives in the Examiner Interview held on April 18, 2007 at the USPTO. In the interview, the Examiner stated that the meaning of the claim term "graphical password" was not clear. Independent claims 1, 7, 23, 29, 47 and 54 have been appropriately amended to give proper definition to the claim term "graphical password." It is respectfully submitted that the term "graphical password" is well known in the art and the inclusion of definition to that term does not constitute new matter. Please refer to the background section of the application, including paragraph [0007].

## GROUNDS FOR ENTRY OF THIS RESPONSE PURSUANT TO 37 C.F.R. 1.116

The Applicants respectfully request entry of this Rule 116 Response because it is believed that the arguments and amendments put forward place these claims in condition for allowance. These arguments and amendments were not earlier presented because the Applicants believed in good faith that the cited prior art did not disclose the present invention as claimed.

## CLAIM REJECTIONS

Claims 1-55 were rejected under 35 USC 102(b) as being anticipated by Sugimura et al. (US 2003/0115473) (hereinafter "Sugimura").

### Claims 1-6 and 45

Amended claim 1 recites: "...determining whether to authenticate the user depending on whether the extent to which a location of the input graphical password matches with a reference location of a registered graphical password is within an authentication margin for a location of any input graphical password with respect to the reference location of the registered graphical password..." In claim 1, a user is first authenticated depending on whether the extent to which a location of the input graphical password matches with a reference location of a registered graphical password is within an authentication margin for a location of any input graphical password with respect to the reference location of the registered graphical password. If the user is not authenticated, a graphical password input history is stored.

However, in contrast to claim 1, according to paragraph [0035] of Sugimura, a user is first authenticated using a password or a digital certificate, namely, maybe a combination of characters and numbers, not a graphical password. The cited reference does not disclose comparison of graphical password locations and storage of a graphical password input history.

Claim 1 has been amended to include the definition of the claim term “graphical password” as a predetermined graphical image on a display where the user selects predetermined areas of the graphical image in a predetermined sequence. Support for this amendment may be found in at least paragraph [0007] of the present application.

Claims 2-6 depend on claim 1 and are therefore believed to be allowable for at least the foregoing reasons. Further, claim 45, which recites a computer readable medium to enable the method of claim 1, is also believed to be allowable for the foregoing reasons.

Withdrawal of the foregoing rejection is requested.

**Claims 7-22**

Amended claim 7 recites: “...authenticating the user based on a result of comparing the user’s biometrics information with registered biometrics using the set threshold biometrics value.” Claim 7 pertains to performing biometric authentication after the graphical password matching. Specifically, the biometric authentication is performed unconditionally. However, Sugimura pertains to registering and storing the user’s biometric information only when the user is authenticated to be authorized. Namely, when the user fails to be authenticated, the user does not have a chance to perform the biometric authentication, as is recited in claim 7.

Claims 8-22 depend on claim 7 and are therefore believed to be allowable for at least the foregoing reasons. Further, claim 46, which recites a computer readable medium to enable the method of claim 7, is also believed to be allowable for the foregoing reasons.

Further, claim 7 has been amended to include the definition of the claim term “graphical password” as a predetermined graphical image on a display where the user selects predetermined areas of the graphical image in a predetermined sequence. Support for this amendment may be found in at least paragraph [0007] of the present application.

Withdrawal of the foregoing rejection is requested.

**Claims 23-28**

Amended claim 23 recites: "...a control unit which authenticates the user depending on whether the extent to which a location of the input graphical password matches with a reference location of a registered graphical password is within an authentication margin for a location of any input graphical password with respect to the reference location of the registered graphical password." Claim 23 recites a control unit to perform biometric authentication after the graphical password matching. Specifically, the biometric authentication is performed unconditionally. However, Sugimura pertains to registering and storing the user's biometric information only when the user is authenticated to be authorized. Namely, when the user fails to be authenticated, the user does not have a chance to perform the biometric authentication, as is recited in claim 23.

Further, claim 23 has been amended to include the definition of the claim term "graphical password" as a predetermined graphical image on a display where the user selects predetermined areas of the graphical image in a predetermined sequence. Support for this amendment may be found in at least paragraph [0007] of the present application.

Claims 24-28 depend on claim 23 and are therefore believed to be allowable for at least the foregoing reasons.

Withdrawal of the foregoing rejection is requested.

**Claims 29-44**

Amended claim 29 recites: "...a biometrics unit which authenticates the user based on a result of comparing the user's biometrics information input from the outside with registered biometrics." Claim 29 recites a biometrics unit to perform biometric authentication after the graphical password matching. Specifically, the biometric authentication is performed unconditionally. However, Sugimura pertains to registering and storing the user's biometric information only when the user is authenticated to be authorized. Namely, when the user fails to be authenticated, the user does not have a chance to perform the biometric authentication, as is recited in claim 29.

Further, claim 29 has been amended to include the definition of the claim term "graphical password" as a predetermined graphical image on a display where the user selects predetermined areas of the graphical image in a predetermined sequence. Support for this amendment may be found in at least paragraph [0007] of the present application.

Claims 30-44 depend on claim 29 and are therefore believed to be allowable for at least the foregoing reasons.

Withdrawal of the foregoing rejection is requested.

**Claims 47-51**

Amended claim 47 recites: "...adjusting the predetermined proximity window, wherein the predetermined proximity window is decreased when the invalid result is output." In contrast to claim 47, Sugimura does not disclose decreasing a proximity window, or any feature similar.

Claim 47 has been amended to include the definition of the claim term "graphical password" as a predetermined graphical image on a display where the user selects predetermined areas of the graphical image in a predetermined sequence. Support for this amendment may be found in at least paragraph [0007] of the present application.

Claims 48-51 depend on claim 47 and are therefore believed to be allowable for at least the foregoing reasons.

**Claims 52 and 53**

Claims 52 and 53 have been cancelled.

**Claims 54 and 55**

Amended claim 54 recites: "...a biometrics unit which reads the user's biometrics information and authenticates the user based on a result of comparing the user's biometrics information with the registered biometrics using the set threshold biometrics value." Claim 54 recites a biometrics unit to perform biometric authentication after the graphical password matching. Specifically, the biometric authentication is performed unconditionally. However, Sugimura pertains to registering and storing the user's biometric information only when the user is authenticated to be authorized. Namely, when the user fails to be authenticated, the user does not have a chance to perform the biometric authentication, as is recited in claim 54.

Further, claim 54 has been amended to include the definition of the claim term "graphical password" as a predetermined graphical image on a display where the user selects predetermined areas of the graphical image in a predetermined sequence. Support for this amendment may be found in at least paragraph [0007] of the present application.

Claim 55 depends on claim 54 and is therefore believed to be allowable for at least the foregoing reasons.

Withdrawal of the foregoing rejection is requested.

**CONCLUSION**

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: May 7, 2007

By: / Gregory W. Harper /
Gregory W. Harper
Registration No. 55,248

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501